Remarks/Arguments

Claims 1-7 are pending. Claims 1-7 stand rejected. Reconsideration of this application is requested.

Response to Arguments

Applicant notes the Examiner's statement on page 2 of the present Office action that:

> In response to Applicant's argument that the references fail to show certain features of applicant's invention, it is noted the certain features upon which applicant relies (i.e. generating a scambling key in (emphasis added) a smart card using a first seed value received by the smart card and a second seed value permanently stored in the smart card, and thus fails to render claim 1) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims.

In response, Claim 1 has been amended to more clearly recite that the scrambling key is generated in the smart card. Support for this amendment may be found within the specification, on page 6, in lines 5-9, for example, wherein it recites, "[t]he scrambled A/V signal and the second seed value is received by DTV 40 and is coupled to SC 42 for processing. SC 42 receives the second seed value and utilizes both the stored first seed value and the received second seed value to reconstruct (or recover) the symmetric key."

Applicant notes this amendment should not raise any new issues of patentability, as Claim 5 already recites:

> (c) coupling said scrambled signal and said first seed value, both received from the service provider, to said smart card, said smart card having a means for access control processing; said access control processing means comprising means for generating said scrambling key... (emphasis added)

Applicant further notes that Shamir expressly teaches against permanently storing any key share in the signature generating device. See, *e.g.*, col. 2, lines

42-44 ("*The device does not contain any secret information and thus it need not be be protected against inspection.*") The Shamir reference clearly teaches against storing any key share in the signature generating device. Accordingly, the teachings of Shamir are expressly inconsistent with the limitations of Claim 1 (and of Claim 5) that permanently stores one of the key shares in the smart card that ultimately generates a key using those key shares.

Instead, Shamir teaches storing each of the key shares on like magnetic cards, each of which is given to an individual (such as a company executive). *See, e.g., col. 2, lines 38-39.* It is improper to equate one of the shares being stored in one of these like cards to the recited permanently stored key share of Claim 1, and another to the received key share of Claim 1. Such interpretation is improper at least because: (1) none of these key shares are stored in the machine that ultimately uses the key shares (*e.g.*, the Shamir signature generating machine), and (2) all of the key shares are stored on like magnetic cards, and hence, are all received by the machine that uses the key shares (*e.g.*, the Shamir signature generating machine).

In view of the foregoing amendment and remarks, Applicant respectfully requests reconsideration and allowance of present Claims 1-7.

35 U.S.C. 103(a) Rejections

Claims 1-7 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Chaney in view of Shamir. This rejection is respectfully traversed, as the combination of Chaney and Shamir fails to teach or suggest each of the limitations recited in Claims 1-7.

The present invention employs the concept of secret sharing which eliminates the requirement for using public key cryptography to ensure secure transmission of the audio/video stream from a service provider (page 5, lines 4-7). A first seed value received in a smart card, and a second seed value permanently stored in the smart card are used to generate a symmetric key in the smart card (page 5, line 31 - page 6, line 20). Accordingly, Claim 1 recites in part:

> (c) generating, in said smart card, said scrambling key using said first seed value and a second seed value in a predetermined function, whereby

> secret sharing is implemented, said second seed value being permanently stored in said smart card

Similarly, independent Claim 5 recites:

> calculating the Y-intercept of a line on said Euclidean plane by said first seed value and a second seed value which is permanently stored in said smart card and means for descrambling, whereby secret sharing is implemented, within said smart card.

No combination of Chaney with Shamir teaches or suggests the above-identified features and limitations. Chaney teaches a system that uses first and second smart cards to produce an image that includes multiple image portions, such as picture in picture (PIP) or picture outside picture (POP). In this regard, the Chaney reference uses entitlement management messages (EMMs) and entitlement control messages (ECMs), which are transmitted with the digital video stream, to control access to the video programs.

The EMM indicates entitlement to a particular service, *e.g.*, all programming on a particular channel, or to a particular program offered by a service, *e.g.*, one movie on a particular channel (col. 2, lines 55-60). The ECM data is used to generate a descrambling key after entitlement to the program has been verified. The ECM provides initialization data for key generation routines that are executed by the processor (col. 2, lines 61-67; col. 4, lines 12-14; col. 7, lines 12-16).

The ECM may be transmitted in encrypted form, in which case, the smart card must first descramble the ECM to derive the initialization data that is used to generate the descrambling key. The key for descrambling the ECM may be stored on the smart card when the card is issued to the user (col. 10, lines 40-47).

In this case, it is clear that a first key received by the smart card, and a second key stored in the smart card, according to Chaney, cannot be understood to correspond to the first and second seed values recited in the present claims. According to Chaney, the key stored in the card is used to descramble the ECM, which is then used to generate initialization data. Even if one were to equate this initialization data to the claimed key received in the card, one must note the initialization data is used in an entirely different algorithm than the key stored in the card. That is, the stored key is used to derive the initialization data, which is in turn used to derive the descrambling key with another algorithm.

In contrast, Claim 1 recites using both the stored key **and** the received key in a predetermined function, whereby secret sharing is implemented. Independent Claim 5 recites calculating a Y-intercept using the first and second seed values. Chaney does not teach or suggest using a stored key **and** a received key in a predetermined function. Chaney teaches no such approach. Rather, the key stored in the Chaney smart card is used to acquire the initialization data, and is not used with the initialization data, as required by Claims 1 and 5.

Shamir fails to overcome the deficiencies of the Chaney reference. As discussed above, Shamir expressly teaches against storing any key in the device that uses the key, no less using a key stored in the device with a received key (*e.g.*, the Shamir signature generating device or present smart card). Accordingly, Shamir also fails to teach or suggest using a received key **and** a key permanently stored in a key generating device in a predetermined function. Thus, the proposed combination of Chaney and Shamir fails to teach or suggest each of the features and limitations recited in Independent Claim 1 (and Claim 5).

In summary, the Chaney reference merely teaches using a key stored in a smart card to derive initialization data, and then using the initialization data to derive a descrambling key, while Shamir teaches using key shares stored on like magnetic cards for insertion into a separate signature generating device (that does not store any key shares), in order to generate a signature. Combining these teachings fails to arrive at applicant's claimed invention of:

> A method for managing access to a signal representative of an event of a service provider, said method comprising:
> (a) receiving said signal in a smart card, said signal being scrambled using a scrambling key;
> (b) receiving, in said smart card, data representative of a first seed value;
> (c) generating, in said smart card, said scrambling key using said first seed value received in said smart card and a second seed value in a predetermined function, whereby secret sharing is implemented, said second seed value being permanently stored in said smart card; and
> (d) descrambling, in said smart card, said signal using said generated scrambling key to provide a descrambled signal. (emphasis added)

In view of the foregoing, reconsideration and withdrawal of this 35 USC 103 rejection is respectfully requested.

The above notwithstanding, Applicant submits that the proposed combination of Chaney and Shamir is improper because neither reference teaches or suggests a motivation for combining the references in the manner suggested by the Examiner.

First, Chaney and Shamir describe entirely different methods for generating a descrambling key or desired function. Neither reference teaches or suggests how such a proposed combination of methods might operate, or even why it would be desirable to modify the primary reference of Chaney in the manner argued in the Final Office action.

Examiner reasons that a proper motivation to combine the reference lies in: 1) Shamir's alleged teaching that "dividing the key into pieces and distributing the key provides a robust key management system"; and 2) Shamir's alleged teaching that "[t]his would also decrease fraud because an unfaithful executive must have at least two accomplices in order to forge the company's signature scheme." (see page 3, last para. of Final Office action).

In response, Applicant submits that the Examiner has failed to articulate any rationale as to how the Shamir key sharing scheme, designed to prevent an unfaithful executive from forging a company's signature (for signing checks), relates in any way to the video signal processing scheme of Chaney (or the method of the presently claimed invention) for managing access to a signal representative of an event of a service provider and system for managing access between a service provider and a device. Neither the references themselves, nor the present rejection as articulated, provides any basis or motivation to modify the video processing scheme of Chaney with a process for preventing an unfaithful executive from forging a company's signature in an attempt to reach the claimed invention. Chaney makes no mention of the problem solved by the Shamir reference as it relates to Chaney's video signal processing scheme. Similarly, Shamir itself fails to teach or suggest video signal processing at all, and instead

teaches a particular key management threshold scheme as it relates to check signing.

Still further, modifying the video system of Chaney to incorporate the threshold approach of Shamir as argued by the Examiner, nevertheless results in a system that does not store any secret data, such as key shares, in the device that generates a key ("The device does not contain any secret information and thus it need not be protected.") Accordingly, one is required to further modify the asserted Chaney/Shamir approach to store a key share in the signature generating device to reach the claimed limitation of "generating, in said smart card, said scrambling key using said first seed value and a second seed value in a predetermined function, whereby secret sharing is implemented, said second seed value being permanently stored in said smart card." However, such a further modification finds no basis in the references themselves, and, is in fact entirely inconsistent with: (1) the express teachings of Shamir ("the device does not contain any secret information"); and (2) the Examiner's asserted motivation for combining these references, namely, "to provide a more robust key management system", as storing a key in the signature generating device, even if itself secured, is necessarily less secure than not storing a key in the device in the first place.

In view of the above, Applicants respectfully submit that the suggested combination of Chaney and Shamir is improper and constitutes impermissible hindsight gleaned from Applicant's own specification. For this additional reason, reconsideration and withdrawal of this rejection is requested.

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicants' attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,
A. Eskicioglu, et al.

By: Paul P. Kiel
Attorney for Applicants
Registration No. 40,677

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312

Date: September 9, 2005

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being transmitted via facsimile to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 2313-1450 on September 9, 2005 at facsimile number (571) 273-8300.

September 9, 2005
Date

By: Eliza Buchalczyk